文章编号:1671-4598(2024)04-0314-08 DOI:10.16526/j.cnki.11-4762/tp.2024.04.044 中图分类号:TP206+.3 文献标识码:A

基于 MBSE 的鱼雷全电子安全系统安全性与任务可靠性分析

王储炘[1]，秦栋泽[1]，刘 瑜[2]
(1. 中北大学 机电工程学院，太原 030051；2. 中船西安东仪科工集团有限公司，西安 710065)

摘要：随着武器装备研究的深入推进，传统方法难以满足复杂系统安全性与可靠性分析的需求；为提升系统研发与评估效率，以形式化的系统建模语言分析鱼雷全电子安全系统的安全性、可靠性成为必然趋势；文章在传统安全性与可靠性分析的基础上，基于系统工程开展安全系统建模过程，以功能需求、系统架构、活动视图以及时序逻辑控制作为安全性与作用可靠性分析的构成元素，对系统功能模型进行故障传播建模；最后以安全建模语言构建事故树模型得出安全性与可靠性的影响因素，为引信系统的安全性与可靠性分析工作提供一定参考价值。

关键词：引信；鱼雷；全电子安全系统；安全性；可靠性；MBSE

Safety and Mission Reliability Analysis of Torpedo Electronic Safety and Arming System Based on MBSE

WANG Chuxin[1], QIN Dongze[1], LIU Yu[2]
(1. College of Mechatronics Engineering, North University of China, Taiyuan 030051, China;
2. Xi'an DongYi Science Technology & Industry Group Co., Ltd.,
China State Shipbuilding Corporation Limited, Xi'an 710065, China)

Abstract: With the deepening of research on weapons and equipment, traditional methods are difficult to meet the analysis needs of safety and reliability in complex systems. In order to improve the efficiency of system development and evaluation, it is an inevitable trend to analyze the safety and reliability of torpedo electronic safety and arming system with formal system modeling language. Based on the traditional reliability analysis of the security system structure, this paper carries out the corresponding system modeling process based on system modeling language (SysML), and takes the functional requirement, system architecture, activity view and temporal logic control as the constituent elements of the security and action reliability analysis to model the fault propagation of the system functional model; Finally, the tree model of accident is constructed with the safety modeling language to obtain the influencing factors of reliability, and it provides a certain reference value for the safety and reliability analysis of fuze systems.

Keywords: fuze; torpedoes; electronic safety and arming system; safety; reliability; model-based systems engineering (MBSE)

0 引言

以电子信息技术为关键推动力的技术革新不断发展，现代装备体系表现出自动化、智能化的特点。随着先进技术的快速发展并广泛应用于军事武器装备中，对现代武器系统的效能、系统的结构复杂度、环境适应性以及不可预见性等特性越发显著，对引信战术技术，包括安全性、可靠性进行科学可靠的分析评估提出了更高的要求。

全电子安全系统控制引信以探测到的环境信息和内部指令使其从安全状态转换成待发状态，并能可靠地解除保险[1]。相较于传统机械安全系统，全电子安全系统测量方法有一定局限性，即系统状态变量不可观测，仅能通过输出体现[2]。鱼雷的复杂工作环境对引信能够可靠解除保险的能力要求更高，基于电子技术的全电子安全系统既要保证引信全弹道设计上对己方具有高安全性，又要保证目标作用的高可靠性。对于引信系统设计与分析，文献[3]对全电子安全系统解除保险逻辑进行了对比，分析得出一种高安全性的设计方法；文献[4]采用故障树分析法对引信作用可靠性进行了分析，得出引信定性定量分析结果；文献[5]对6种系统可靠性分析方法从适用范围、输入输出和优缺点进行了对比分析。

目前引信安全系统安全性与可靠性的分析方法主要有故障树分析方法（FTA，fault tree analysis）以及失效模式影响与危害分析（FMEA，failure mode and effect analysis），主要依赖于分析人员的知识、经验，人为差异可能会造成错、漏事件发生。且以文本形式表示故障信息不精确、更新不及时，传统分析方法会造成安全性与可靠性分析存在功能定义上的错误，边界确立的模糊歧义，难以保证分

收稿日期:2023-09-14； 修回日期:2023-10-07。
作者简介:王储炘(1998-),男,硕士研究生。
引用格式:王储炘,秦栋泽,刘 瑜.基于 MBSE 的鱼雷全电子安全系统安全性与任务可靠性分析[J].计算机测量与控制,2024,32(4):314-321,340.

析与设计工作的一致性。

MBSE 运用系统建模语言（SysML，system modeling language）进行系统架构分析与设计，从需求、结构和行为的视图上对安全系统架构创建功能元素与物理组件的映射关系[6]。目前，MBSE 在国内外航空、武器领域成为系统设计与分析的主流发展趋势之一。由其衍生的基于模型的安全性与可靠性分析相较于传统的文档分析方法，解决了信息化研发技术在处理系统需求、整体架构方面的欠缺[7]。实现 MBSE 在系统设计的同时兼顾安全性与可靠性的评估验证工作需要。文献［8］对国内外基于模型的系统安全性与可靠性分析研究进展做出介绍，对该技术的优势、应用趋势进行了探讨，并指出应进一步完善该方法在安全性、可靠性建模规范体系的建立；文献［9］围绕功能逻辑模型进行可靠性、安全性和测试性“三性”建模评估方法；文献［10］基于 SysML 多视图模型构建描述导弹系统任务剖面以及安全性研究，构建完整的系统建模分析过程；文献［11］对卫星系统自身的运行状态和单元故障之间的时序关系与逻辑相关进行刻画，以模型方式构建系统故障模式。引入工程系统角度研究安全系统安全性与可靠性的方法，适应当前引信系统数字化设计趋势，同时基于模型方法，能够使系统的故障规律得到清晰的体现[12]。

1　安全系统故障分析理论基础

作为鱼雷引信的主要安全装置，ESA 由逻辑控制部分与起爆控制电路组成。以模块方式建立引信系统架构，将引信结构中的逻辑控制模块与起爆控制整合为安全起爆系统，起爆控制指令由控制模块内部总线进行传输。逻辑控制部分由两个独立控制的集成电路模块、冗余开关构成，分别受不同的环境信号影响实现解除保险的动作，满足引信安全性设计要求[13]。ESA 的逻辑控制部分采取时序控制、时间窗控制等技术，提高引信安全性。由电子元件组成的引信系统保证了高可靠性。鱼雷全电子安全系统原理如图 1 所示。

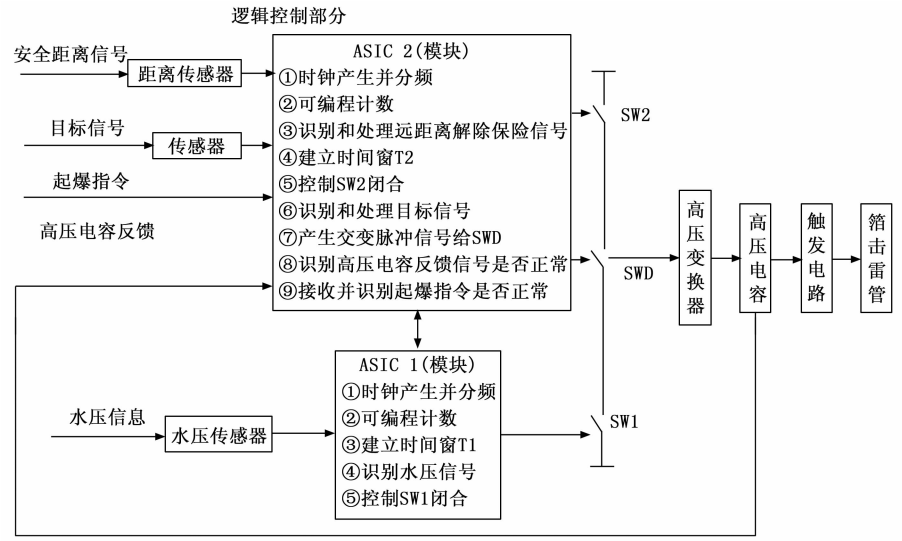

图 1　鱼雷全电子安全系统原理框图

引信在结构上尽管规模不大，亦适用系统整体研究方法进行设计与安全性分析。文献［14］引入工程系统角度研究引信安全性与可靠性权衡问题。通过数字化的建模方法设计引信故障分析方案，创建出结构良好且清晰的模型，将文档中描述系统结构、功能、性能等方面转化为规范化的可交互的仿真验证流程[15]。在规范化建模过程下，能够有效规避分析中存在功能定义上的错误、边界确立的模糊歧义，保证分析工作的一致性。本文引入 MBSE 设计思想实现鱼雷全电子安全系统安全性与任务可靠性分析，运用系统整体建模的概念对引信全电子安全系统的安全性、可靠性的需求进行剖析。通过对系统功能模型进行验证，推测任务可靠性分析过程中可能出现的故障，从而得出故障发生的过程与造成故障产生的具体因素[16]。

2　任务需求分析

全电子引信产生起爆战斗部动作，控制引信以预定的环境信息或鱼雷内部指令使其从安全状态转换成待发状态时，应可靠地解除保险。解除保险的条件在自然状态下难以发生，因此本文对系统安全性与可靠性分析的场景为鱼雷发射后的水下工作过程。通过对系统需求的剖析与整合，以 ESA 任务需求、功能需求与各部分组件设计要求为导向，将系统功能故障处理作为安全性与可靠性分析工作重点。将鱼雷安全系统发射入水后的解保过程作为系统安全性与可靠性分析的场景。

将鱼雷引信全电子安全系统任务设为顶层设计需求，建立需求模型表示安全性需求与可靠性需求之间的关系，进行相关使命任务分析，并构建需求模型[17]。以全电子安全系统任务构建需求模型进行相关使命任务分析，将系统功能需求转化为系统边界。

鱼雷武器引信系统主要有以下分任务需求：

1）作用可靠性需求：作用可靠性是指在规定的环境条件和时间内，引信能够达成指定功能的性能。代表对系统处理任务要达到的要求。系统接收到爆炸指令可有效运行，保证作战任务成功完成。指在规定的环境条件和时间内，引信能够达成指定功能的性能。鱼雷发生早炸、迟炸、自毁失效以及瞎火故障，均是引信作用可靠性未完成的表现。

2）安全性需求：安全性需求为保证系统在规定条件下不意外解除保险或爆炸的功能要求；全电子安全系统最少有两个独立的保险件，每个都可避免引信意外解除保险，同时多保险的激励条件需为不同的环境条件，通过利用侦测到的环境信息和目标信息进行开关解保，解除隔爆状态。安全系统采用“阈值＋顺序＋时间窗”的判断方法辨明接收的信号，在规定的时间内信息识别电路必

须正确识别环境信号，判断阈值、出现时间和持续宽度是否满足条件。

3 逻辑架构分析

为引信安全系统构建鱼雷入水与目标毁伤段的逻辑架构，进行功能与行为的分解。针对安全系统系统的各级子系统的需求建模顶层子系统，将参数定义至对应的包中，根据行为间交互构建不同子系统之间的流关系与接口。

3.1 系统结构分析

SysML 中的模块定义图（BDD，block definition diagram），注重于刻画系统及元素结构的模块化单元[18]。通过构建 SysML 块定义图，由 BDD 描述安全系统整体架构信息，从而建立全电子安全系统组成元素、各个模块之间的接口以及各个组件之间的相互关联、作用的方式。通过对安全系统结构与属性进行建模，定义安全系统的价值属性、组成属性、约束属性、将系统分解为若干子系统构成的统一整体。安全系统整体架构模型如图 2 所示。

全电子安全系统采用基于目标基解除保险的方式，将安全状态转换为解除保险状态。传感器向控制芯片发送环境信息，控制 1、2 级静态开关与动态开关的闭合状态。系统对时序进行控制，利用异常处理模块对信息正确性与开关闭合状态进行识别与监测，进一步采取复位等恢复操作。发火控制装置由高压转换器、高压电容、发火电路和箔击雷管构成。高压起爆电路控制电压由低压向高压转换，完成高压电容充电动作，使引信解除能量隔爆进入待发状态。

3.2 内部结构分析

内部模块图（IBD，internal block diagram）用于和模块定义图互相补充信息，结合系统整体架构显示模块间彼此调用的服务。以图 3 示例，建模 ASIC Ⅰ芯片控制电路内

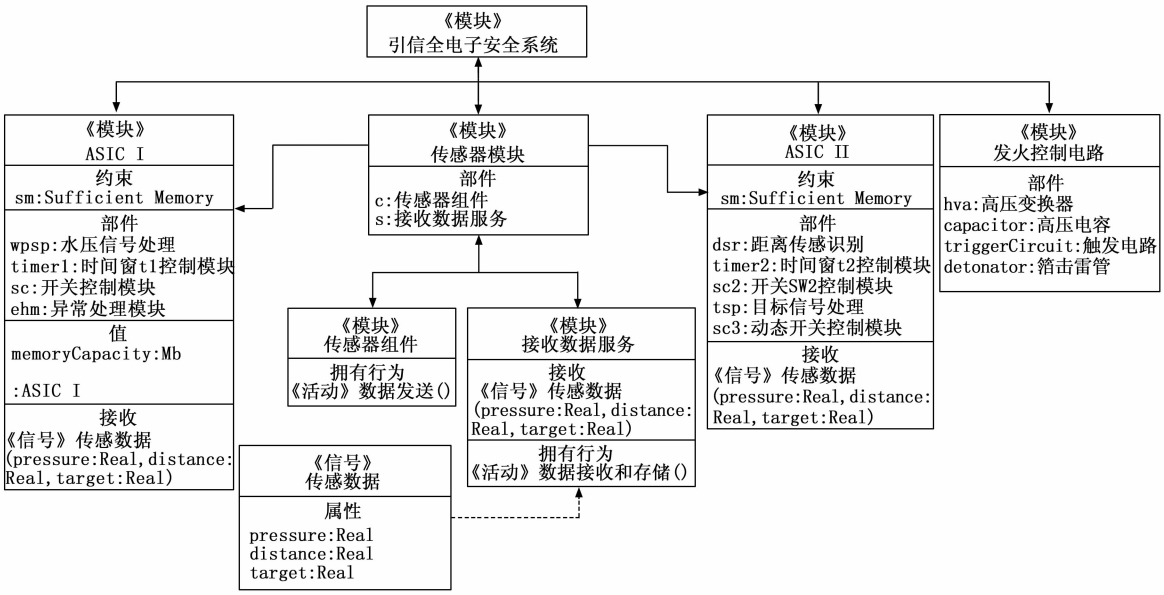

图 2 安全系统架构模型

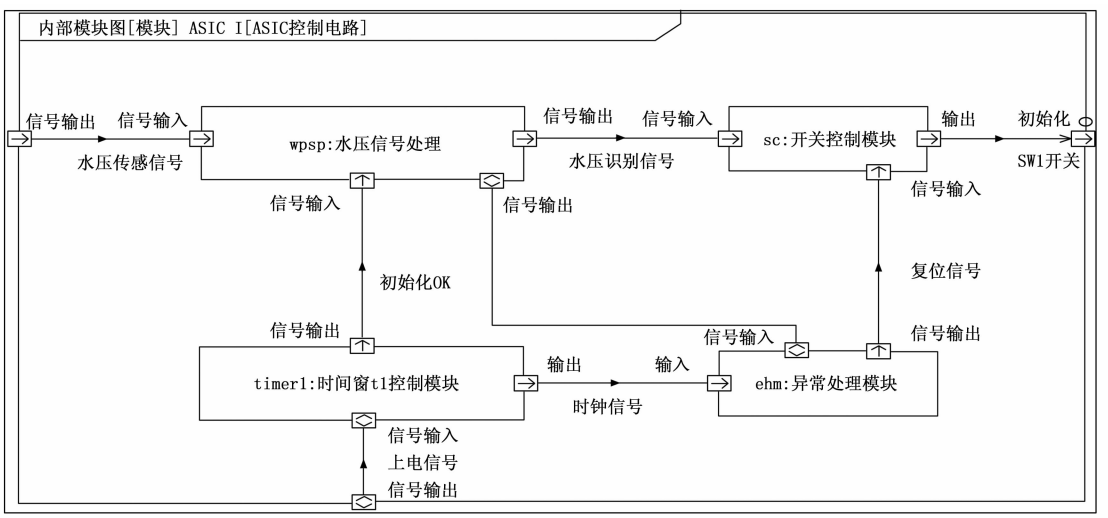

图 3 ASIC Ⅰ内部模块图

部模块图，显示框图内部连接关系与外部输出。根据功能模块部件连接关系，通过内部总线和信号传输端口进行信号导出系统内部信号传递关系。根据 IBD 制定模块的内部结构，显示子系统属性、端口、项目流等结构特性。通过内部块图的描述，将电路内部的信号传递转换为可视的行为状态模型。

3.3　系统时序建模

运用 SysML 构建的全电子安全系统时序图，纵轴表示对象，消息在各对象之间横向传递，依照时间顺序描述执行系统功能的各个角色之间传递消息的顺序。图 4 为入水状态下安全系统的运行流程。

ESA 以鱼雷发射入水为计时零点，系统上电并完成初始化、自检测功能，安全系统根据所接收的环境信息对各阶段保险进行解保操作。通过时序图梳理开关解保过程，以消息传递的形式通过时序状态分析得出多个对象之间的动态协作关系，对安全系统的时序逻辑进行建模。

3.4　作用活动建模

对系统逻辑单元中各部分活动的行为建模。通过构建活动图的方式，按执行功能的不同划分泳道构建动作状态、对象流描述系统行为导致对象状态改变的结果，如图 5 所示。

系统的使用场景和操作取决于引信的任务类型、任务剖面以及每个任务剖面下引信系统的操作程序，采用活动图从顶层描述 ESA 的任务使命、任务剖面和主要任务阶段，分析安全系统相关的操作场景；利用场景模型识别出系统的主要功能。在运行过程中通过活动图行为模型边框

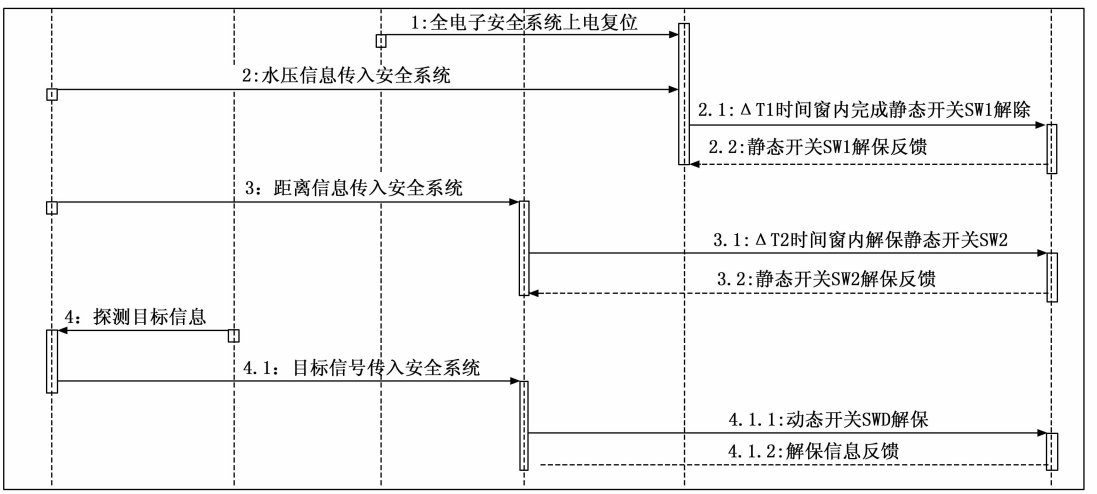

图 4　鱼雷全电子安全系统时序图

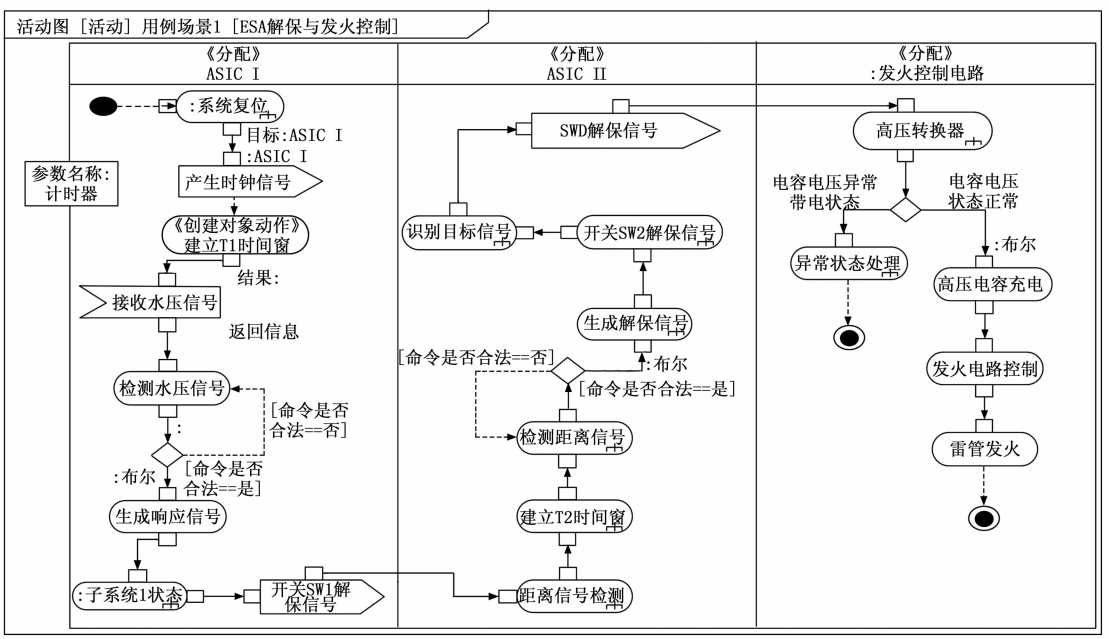

图 5　安全系统作用活动模型

颜色变化进行过程验证，观察信号在系统中的流动变化以及内部动作的交互，确保故障－功能耦合定义的正确性。

3.5 系统状态建模

创建系统在工作周期内的动态行为状态模型，表示系统状态变化，确定产生运行状态转变的进入、持续与状态退出动作。解保顶层状态模型将安全系统工作过程分解为引信入水检测、加电、信号识别、处理、复位、解保控制 5 种状态，各状态间以环境信息作为状态转换条件，建立引信安全系统工作过程描述，如图 6 所示。

以安全系统解除保险状态为用例场景的子系统状态图为载体，显示引信安全系统关键属性并确定系统状态。将接收信息、输出状态转换后的处理信号设置为状态转移的触发条件，完成具体指令进行状态的串行变化的仿真验证。异常状态下，当环境信息错误及电路状态发生故障时，应转入故障处理状态，进行系统复位或绝火操作。

4 故障模型分析

4.1 故障模式分析

以白盒分析方法分析系统功能故障，系统功能与潜在故障失效之间影响关系用模块形式表征。如图 7 所示，通过模块定义图表示安全系统功能层次与包含关系，对安全系统按包含关系对功能的父类与子类划分，实现功能内聚模型的构建。

如图 8 所示，根据不同组件功能对故障原型进行划分，创建故障模式架构图，分别创建安全系统的故障及系统故障类型的架构模型。如图所示，左侧对系统组件故障包括传感器故障、控制器故障以及起爆控制电路故障进行划分。右侧定义为引信安全系统模型中的故障类型，以域的形式表示安全性与可靠性的逻辑集合。将系统故障与失效类型用虚线连接，用来表示系统故障与故障类型之间的从属关系，描述各子系统的故障。

全电子安全系统的综合性涉及到集成电路、可编程电子、电气和结构等多个方面的资源。在进行安全性分析时，需要考虑系统架构的约束以及失效模式方面的要求。失效模式是指组件出现故障或失效时，导致系统功能受到影响的模式。一个功能模块可以由多个功能要素组成，而这些要素的组合部分被称为功能要素。在功能故障模型架构的基础上将故障模式与引信系统功能相关联，建立故障可视化模型[11]。追溯矩阵用于对故障状态进行交叉检查，确定两个基线文档之间的关系和完整性，以便在软件仿真过程中确定安全性分析节点。故障与功能的追溯矩阵如图 9 所示。

矩阵行元素代表故障模式，列元素代表引信系统所具有的功能，矩阵中的箭头方向表示将该故障与功能形成完整的耦合关系，数字表示该功能对应受影响故障的数量。引信安全系统的功能为控制三级冗余开关解除保险、进行信息的识别与处理、提供引信复位功能、以及解除保险后的引爆控制。通过追溯矩阵的结果得到系统故障与引信实际功能之间的关联，推导故障影响的功能覆盖范围。

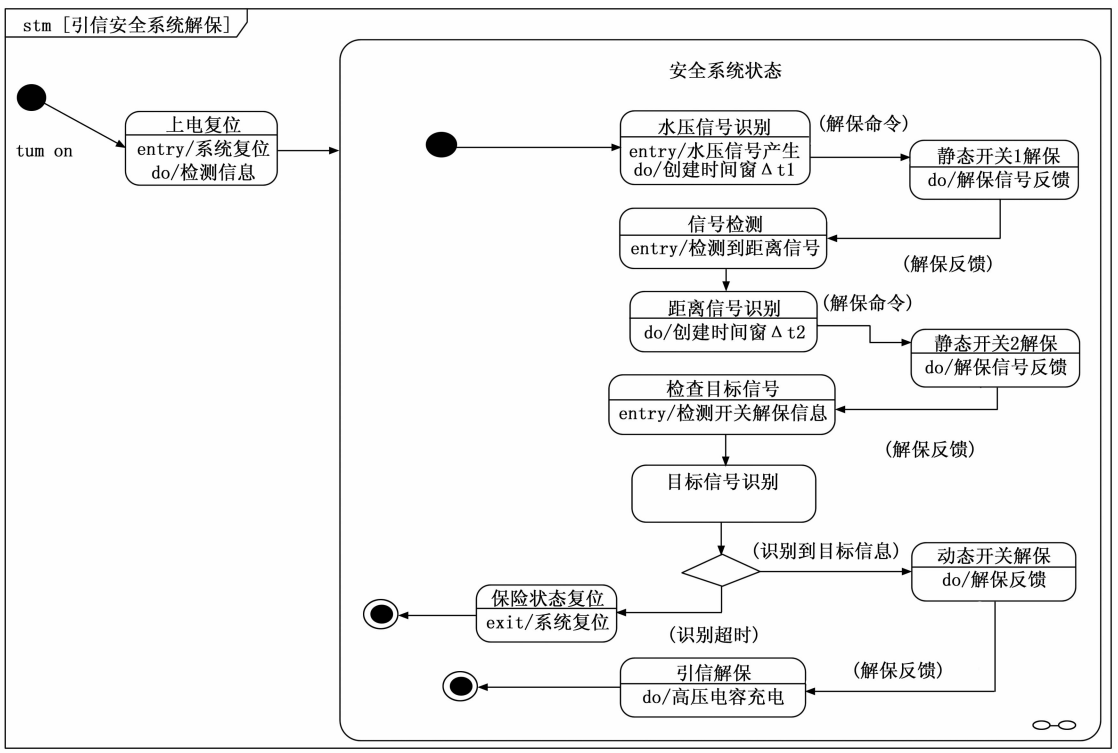

图 6 解保顶层状态模型

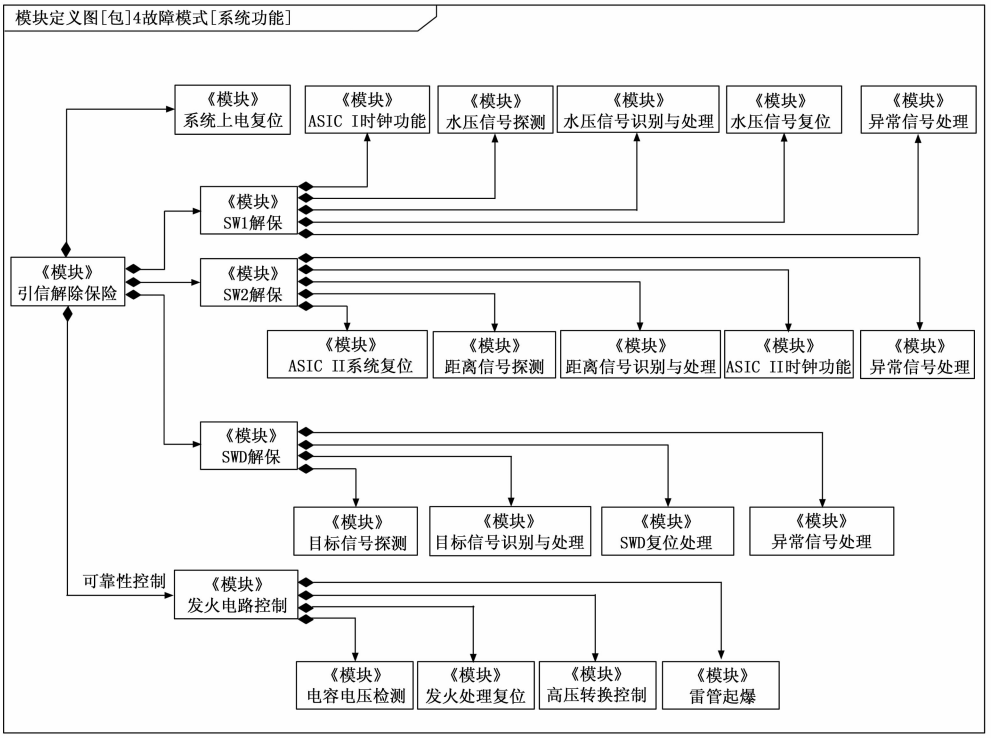

图 7　系统功能分析模型

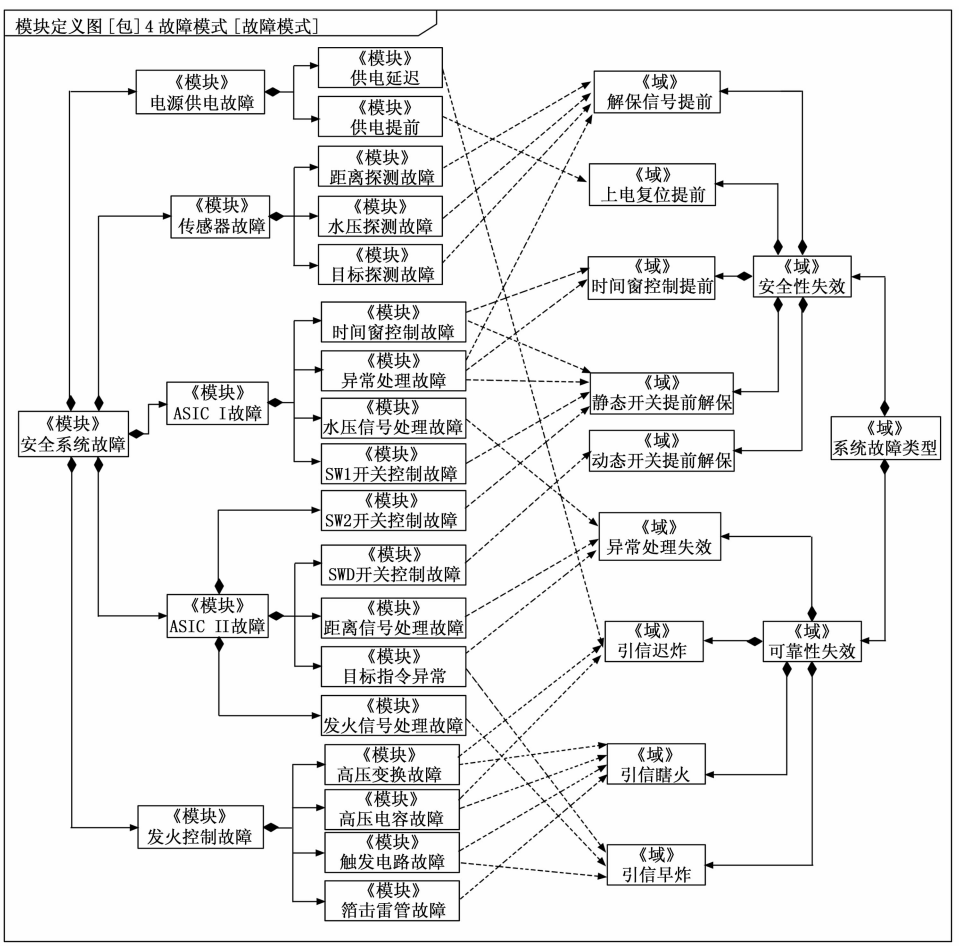

图 8　故障模式架构图

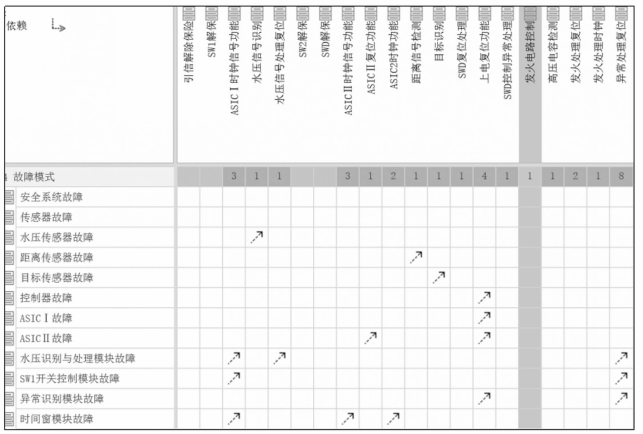

图 9 故障模式与功能追溯矩阵

4.2 故障传播验证

结合上述分析过程，构建出涵盖鱼雷引信全电子安全系统的时序、状态、模块功能、故障模式的系统架构体系，并对系统进行自下而上建模，创建模块内部逻辑与信号传递关系，生成以系统工程为导向的故障传播模型[19]。基于模型的系统化安全性分析模拟工作流程，根据图 10 构建的故障传播模型对安全系统进行运行仿真，通过图形化设计与动态故障注入，验证引信安全系统模型定义的正确性。

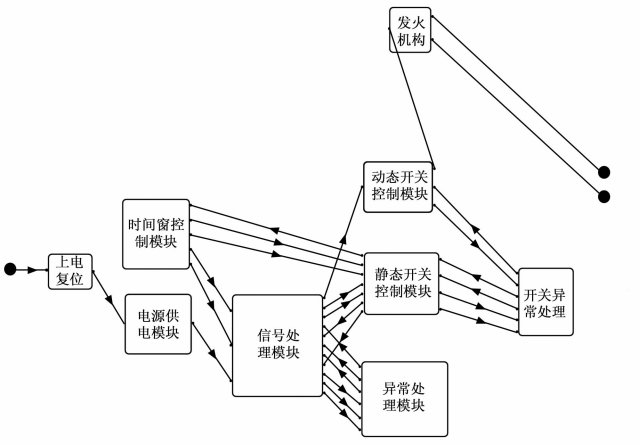

图 10 全电子安全系统故障传播模型

以鱼雷入水时刻作为作用初始节点，以安全系统正常发火控制与异常控制分别为不同的结束节点。矩形块为实现系统功能的模块，内部输入相关功能类型、数据、约束信息和故障传播模式和状态转移模式，对各连接点的逻辑控制关系进行描述；箭头方向代表各模块间信息传递关系；属性定义不同任务阶段的模块状态。对各功能模块间状态转换、信息传递以逐步传播的方式验证系统运行的过程。观测运行时模块故障传播的图像变化形式对中间和最终结果，得出影响引信安全系统安全性与可靠性的组件间的耦合关系。

4.3 故障模式综合分析

通过 SIMFIA 安全性模块制定故障事件规则，对异常交互的行为结合面向故障的安全建模语言 AltaRica，以线性逻辑布尔状态表达式反映输出信号节点与组件状态[20]。根据状态机图中组件行为创建影响系统安全的故障树，当随机事件发生时开关的状态才会发生变化。将影响开关解保信号异常的故障信息以图像化形式展开，完成故障树最小割集和结构重要度的确定，从而对系统故障建模逻辑的正确性进行验证[21]。

在引信安全系统中，不同功能的重要等级有所不同，对系统的影响程度高的部分着重进行分析，作为连接系统安全性与可靠性关键功能的动态开关解保的权重明显较高。由图 11 所示，该故障树的顶事件为“开关 SWD 解保反馈信号.wrong”，引起发生安全性故障的因素可能来源于下方开关解保的每条路径，最终追溯到“目标信号状态错误”。通过对故障树定性分析得出影响安全性与可靠性分析的因素。

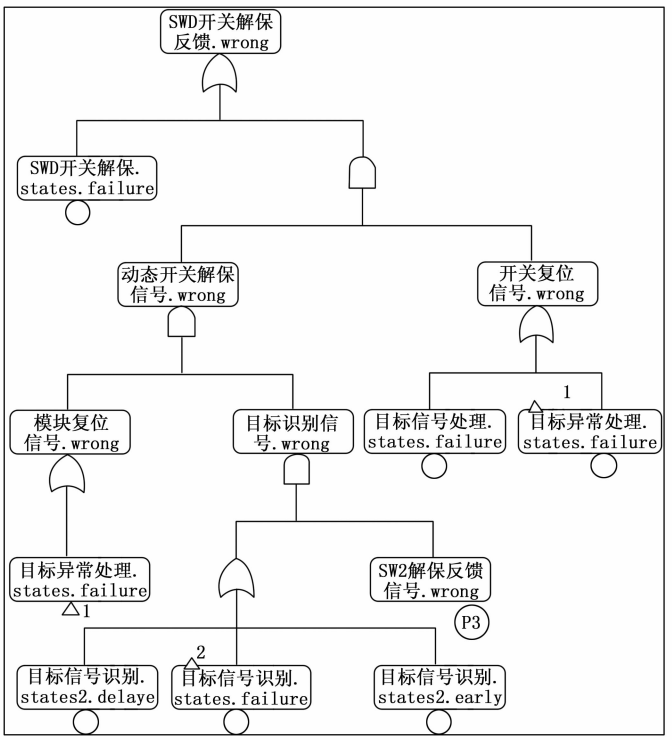

图 11 动态开关解保反馈失效故障树

根据上述分析，由功能—故障模型所生成的故障逻辑关系更加符合现实情况。结合以上视图，以鱼雷引信安全系统故障模式为切入点对安全系统的安全性问题与可靠性问题进行切割，对造成安全系统失效的原因及可能导致的危害和影响建立安全性与可靠性分析表，见表 1、2。分析造成鱼雷可靠性失败的主要因素有：引信提前解除发火保险并发生引爆、延迟发火以及引信瞎火；时序问题、环境信息识别以及开关控制故障，对鱼雷系统作战时己方人员

表 1　鱼雷全电子安全系统安全性分析表

任务剖面：安全系统作用过程任务对象：
全电子安全系统作业流程：ESA 解保过程时序图

#	故障类型	故障失效原因	涉及的故障模式	故障危险后果
1	解保信号提前	水压信号提前	水压信号阈值、特征值识别失效	安全性失效
2		距离信号提前	距离信号阈值、特征值识别失效	安全性失效
3		目标信号提前	目标信号阈值、特征值识别失效	安全性失效
4	时间窗异常	时间窗提前开启	时钟控制异常	安全性失效
5		时间窗失效	时钟晶振异常	安全性失效
6	上电复位异常	上电复位提前	入水信号识别异常	安全性失效
7	开关提前解保	SW1 提前解保	水压信号识别异常	安全性失效
8			水压信号处理异常	安全性失效
9			水压模块探测异常	安全性失效
10		SW2 提前解保	距离模块探测异常	安全性失效
11			距离信号识别异常	安全性失效
12			距离信号处理异常	安全性失效
13		SWD 提前解保	目标信号探测异常	安全性失效
14			目标信号识别异常	安全性失效
15			动态开关解保信号处理	安全性失效

表 2　鱼雷全电子安全系统可靠性分析表

任务剖面：安全系统作用过程任务对象：
全电子安全系统作业流程：ESA 解保过程时序图

#	故障类型	故障失效原因	涉及的故障模式	故障危险后果
1	解保信号延迟	水压信号延迟	水压信号阈值、特征值识别异常	可靠性失效
2		距离信号延迟	距离信号阈值、特征值识别异常	可靠性失效
3		目标信号延迟	目标信号阈值、特征值识别异常	可靠性失效
4		目标识别延迟	目标信号识别异常	可靠性失效
5	上电复位	上电复位延迟	入水信号识别延迟	可靠性失效
6	引信瞎火	电容充电故障	高压转换失效	可靠性失效
7			高压电容充电状态异常	可靠性失效
8		引信上电故障	电源模块失效	可靠性失效
9		未解除隔爆状态	触发电路失效	可靠性失效
10	引信迟炸	目标信息延迟	目标信号控制异常	可靠性失效
11		发火控制延迟	充电状态信号延迟	可靠性失效
12			动态频率信号延迟	可靠性失效
13	引信早炸	发火控制提前	目标信号异常	可靠性失效
14			高压触发信号异常	可靠性失效
15			触发电路异常	可靠性失效
16	异常处理失效	水压模块复位失效	反馈信号处理失效	可靠性失效
17		距离模块复位失效	反馈信号处理失效	可靠性失效
18		目标模块复位失效	反馈信号处理异常	可靠性失效
19		发火控制异常	电压状态反馈失效	可靠性失效

及设备造成危害，导致引信在上电工作后造成安全性问题发生。异常状态处理错误致使不能规避系统错误行为，是造成任务失败的重要原因。

5　结束语

本文针对 ESA 安全性与可靠性分析工作中的边界模糊、系统性不强、可重用性低等问题，利用 MBSE 模型建模移植到引信安全系统安全性与任务可靠性分析工作中。运用系统建模的概念建立引信系统架构，基于功能模型的方式对全电子安全系统的故障模式进行验证，更能体现真实系统的故障传播规律。对于提高鱼雷引信安全系统可靠性，应注意时钟模块与异常处理模块的设计，通过对状态信号处理的用例模拟，优化复位布局布线和复位策略，确定故障处理方案的可行性。

通过该方法将系统工程与鱼雷引信全电子安全系统结合，对运用数字化模型实现引信安全性与可靠性分析进行了实践探讨。结果证明模型驱动方法能够提高系统分析的准确性与效率，可作为相关分析工作的参考，能够为下一步进行可靠性的定量分析提供解决思路。

参考文献：

[1] 甘　雨. 鱼雷引信全电子安全系统保险与解除保险逻辑设计[J]. 鱼雷技术，2012，20（6）：467－471.

[2] 沈　哲. 鱼雷战斗部与引信技术[M]. 北京：国防工业出版社，2009.

[3] 何光林，李　杰，李世义. 基于 3 个环境信号的引信电子安全系统安全性分析[J]. 兵工学报，2002，23（2）：171－175.

[4] 吴进煌，孙少华，曹山根，等. 基于故障树分析法的引信作用可靠性分析[J]. 海军航空大学学报，2022，37（1）：159－164.

[5] 张　伟，贾　瑶. 系统可靠性分析方法与比较研究[J]. 环境技术，2021，39（4）：84－89.

[6] 陈蕊蕊. 基于 SysML 的多域机电产品系统架构建模与校验研究[D]. 杭州：浙江大学，2018.

[7] 陈　磊，焦　健，赵廷弟. 基于模型的复杂系统安全分析综述[J]. 系统工程与电子技术，2017，39（6）：1287－1291.

[8] 胡晓义，王如平，王　鑫，等. 基于模型的复杂系统安全性和可靠性分析技术发展综述[J]. 航空学报，2020，41（6）：140－151.

[9] 李　娇，隆金波，彭文胜，等. MBSE 模式下可靠性安全性测试性一体化建模与评估技术方法[J]. 计算机测量与控制，2021，29（7）：247－253.

[10] 聂兆伟，陈志伟，马晓东，等. 基于多视图建模的武器装备系统安全性分析[J]. 北京理工大学学报，2022，42（4）：437－446.

[11] 种婧宜，周昊澄，袁文强，等. 基于 SysML 的通信卫星故障分析方法研究[J]. 计算机仿真，2022，39（3）：57－61，390.

（下转第 340 页）